

(19) 日本国特許庁 ( J P )

(12) 公表特許公報 ( A )

(11) 特許出願公表番号

特表平10-507324

(43) 公表日 平成10年(1998) 7月14日

(51) Int.Cl. <sup>6</sup>	識別記号	F I
H 0 4 L 9/32		H 0 4 L 9/00 6 7 5 B
G 0 6 F 9/06	5 5 0	G 0 6 F 9/06 5 5 0 E
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00 6 4 0 B
	6 6 0	6 6 0 D

審査請求 未請求 予備審査請求 有 (全 32 頁)

(21) 出願番号 特願平8-509598  
(86) (22) 出願日 平成7年(1995) 9月1日  
(85) 翻訳文提出日 平成9年(1997) 3月5日  
(86) 国際出願番号 P C T / U S 9 5 / 1 1 1 3 6  
(87) 国際公開番号 W O 9 6 / 0 8 0 9 2  
(87) 国際公開日 平成8年(1996) 3月14日  
(31) 優先権主張番号 0 8 / 3 0 3 , 0 8 4  
(32) 優先日 1994年9月7日  
(33) 優先権主張国 米国 ( U S )

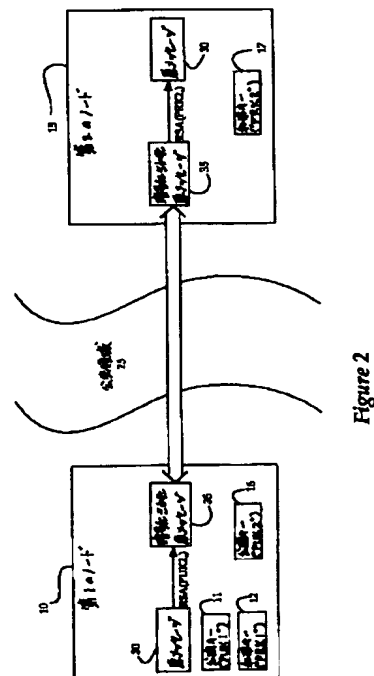
(71) 出願人 インテル・コーポレーション  
アメリカ合衆国 95052 カリフォルニア  
州・サンタ クララ・ミッション カレッ  
シ ブレーバード・2200  
(72) 発明者 デイビス, デレク・エル  
アメリカ合衆国・85044・アリゾナ州・フ  
ェニックス・イースト アシャースト ド  
ライブ・4129  
(74) 代理人 弁理士 山川 政樹 (外5名)

最終頁に続く

(54) 【発明の名称】 ハードウェア・エージェントに対するロビング・ソフトウェア・ライセンス

(57) 【要約】

ライセンス供与制限を強制するための集積回路構成要素。前記強制は、ライセンス・プログラムを実行するアクセス特権を集積回路構成要素から他の同様の構成要素に遠隔送信することによって行われる。集積回路構成要素は、固有に指定されたキーの対 ( 1 1 , 1 2 ) 、認証装置証明 ( 8 0 ) と、製造業者公開キー ( 1 6 ) とを暗号アルゴリズムと共に記憶する不揮発性メモリと、集積回路構成要素に入力された情報を処理するために暗号アルゴリズムを実行し、処理された情報を揮発性メモリに送るプロセッサと、固有に指定されたキーの対を集積回路構成要素内で内部的に生成する乱数発生器とを備える。



**【 特許請求の範囲】**

1. 集積回路構成要素内で情報を処理する処理手段と、

前記処理手段に結合され、集積回路構成要素の製造業者の固有のキー対と認証デジタル証明と公開キーとを記憶する第1の記憶手段と、

前記処理手段に結合され、前記処理手段によって処理された前記情報を記憶する第2の記憶手段と、

前記処理手段に結合され、前記固有のキー対を生成する手段と、

前記処理手段に結合され、前記集積回路構成要素と第2の集積回路構成要素との間の通信を可能にするインタフェース手段とを備える前記集積回路構成要素。

2. 前記第1の記憶手段が不揮発性メモリを含むことを特徴とする請求項1に記載の集積回路構成要素。

3. 前記認証デジタル証明が、前記製造業者の使用キーによって暗号化された前記集積回路構成要素の前記製造業者の前記公開キーであることを特徴とする請求項2に記載の集積回路構成要素。

4. 前記第1の記憶手段が暗号アルゴリズムをさらに含むことを特徴とする請求項2に記載の集積回路構成要素。

5. 前記第2の記憶手段がランダム・アクセス・メモリを含むことを特徴とする請求項1に記載の集積回路構成要素。

6. 前記生成手段が乱数発生器を含むことを特徴とする請求項5に記載の集積回路構成要素。

7. 前記インタフェース手段が、バスに結合されたバス・インタフェースを含み、集積回路構成要素と第2の集積回路構成要素との間に通信リンクを提供して集積回路構成要素が前記第2の集積回路構成要素から集積回路構成要素に送信された情報を復号して記憶し、集積回路構成要素から前記第2の集積回路構成要素に情報を暗号化して送信するようになっていることを特徴とする請求項6に記載の集積回路構成要素。

8. 情報の暗号化と復号を行う集積回路構成要素であって、

固有のキー対と、集積回路構成要素の製造業者の装置証明と、前記製造業者の公開キーとを記憶する不揮発性メモリと、

前記情報を記憶するランダム・アクセス・メモリと、

前記不揮発性メモリと前記ランダムアクセスメモリとに結合され、前記情報を内部的に処理する処理装置と、

前記処理装置に結合され、前記固有のキー対を生成する乱数発生器と、

前記処理装置に結合され、集積回路構成要素が少なくとも第2の集積回路構成要素と通信することができるようにするインタフェースとを備える集積回路構成要素。

9. 前記インタフェースが、集積回路構成要素と第2の集積回路構成要素との間に通信リンクを形成して、集積回路構成要素が集積回路構成要素に送信された情報を復号して記憶し、前記集積回路要素から前記第2の集積回路要素に送信される情報を暗号化して送信することができるようにすることを特徴とする請求項8に記載の集積回路構成要素。

10. ソフトウェア・プログラムを実行するホスト処理手段と、

前記ソフトウェア・プログラムを記憶する記憶手段と、

前記ホスト処理手段と前記記憶手段とを結合するバス手段と、

前記バス手段に結合され、エージェント手段に入力された暗号情報を内部的に復号し、前記エージェント手段から出力される暗号情報を内部的に暗号化する前記エージェント手段と

を備えるシステムであって、

前記エージェント手段は、

前記入力暗号情報および出力暗号情報を前記エージェント内で処理する処理手段と、

前記処理手段に結合され、前記入力暗号情報の復号と前記出力暗号情報の暗号化に使用される、固有のキー対と、前記エージェント手段の製造業者の装置証明と、前記製造業者の公開キーとを記憶する第1の記憶手段と、

前記処理手段に結合され、前記入力暗号情報および出力暗号情報を一時的に記憶する第2の記憶手段と、

前記処理手段に結合され、前記固有のキー対を生成する生成手段と、

前記処理手段に結合され、前記システムと遠隔システムとの間の通信を可能にするインタフェース手段とを含むシステム。

11．前記第1の記憶手段が、不揮発性メモリから電力が切断されても前記固有のキー対を維持する前記不揮発性メモリを含むことを特徴とする請求項10に記載のシステム。

12．前記第1の記憶手段が暗号アルゴリズムをさらに記憶することを特徴とする請求項11に記載のシステム。

13．前期生成手段が乱数発生器を含むことを特徴とする請求項12に記載のシステム。

14．少なくとも1つの暗号化および復号プログラムを記憶する記憶素子と、  
前記暗号化および復号プログラムを実行するホスト・プロセッサと、  
前記ホスト・プロセッサと前記記憶素子とを結合するバスと、  
前記バスに結合され、内部的に前記遠隔装置からの入力情報を復号し、前記遠隔装置への出力情報を暗号化するハードウェア・エージェントとを備えるシステムであって、

前記ハードウェア・エージェントは、

前記ハードウェア・エージェント内で前記入力情報と前記出力情報を処理するプロセッサと、

前記プロセッサに結合され、すべてが前記入力情報の復号と前記出力情報の暗号化に使用される、固有に指定されたキー対と、認証装置証明と、製造業者公開キーとを記憶する不揮発性記憶素子と、

前記プロセッサによって処理された前記入力情報と前記出力情報とを一時的に記憶する揮発性記憶素子と、

前記固有のキー対を生成する乱数発生器と、

前記プロセッサに結合され、前記システムと前記遠隔システムとの間の通信を可能にするインタフェースとを含むシステム。

15. 前記不揮発性記憶素子が少なくとも1つの暗号アルゴリズムをさらに記憶することを特徴とする請求項14に記載のシステム。

16. 1対のハードウェア・エージェントの遠隔識別と認証のための方法であって、

第1のハードウェア・エージェントと第2のハードウェア・エージェントの間に通信リンクを確立するステップと、

前記第1および第2のハードウェア・エージェントを認証するステップと、

前記第2のハードウェア・エージェントが有効なライセンス・トークンを所有しているか否かを判断するために、前記第1のハードウェア・エージェントから前記第2のハードウェア・エージェントに照会メッセージを送信するステップと、

前記第2のハードウェア・エージェントが前記有効なライセンス・トークンを所有している場合に前記第1のハードウェア・エージェントから第2のエージェントへの転送要求メッセージを生成するステップと、

前記第2のハードウェア・エージェントから前記第1のハードウェア・エージェントに前記有効なライセンス・トークンを転送するステップと、

前記有効ライセンス・トークンを受信した後に前記第1のハードウェア・エージェントから前記第2のハードウェア・エージェントへのトークン受信メッセージを生成するステップと、

前記通信リンクを終了するステップとを含む方法。

17. 認証ステップが、

前記第1のハードウェア・エージェントに記憶されている固有の装置証明を前記第2のハードウェア・エージェントに送信するステップと、

前記第1のハードウェア・エージェントと通信し前記第1のハードウェア・エージェントを認証するために、前記固有の装置証明を復号して第1のハードウェア・エージェントの公開キーを入手するステップを含むことを特徴とする請求項16に記載の方法。

18. 認証ステップが、

前記第2のハードウェア・エージェントに記憶されている固有の装置証明を前

記第1のハードウェア・エージェントに送信するステップと、

前記第2のハードウェア・エージェントと通信し前記第2のハードウェア・エージェントを認証するために、前記固有の装置証明を復号して第2のハードウェア・エージェントの公開キーを入手するステップとをさらに含む方法。

19．認証ステップが、

前記第1のハードウェア・エージェントの前記公開キーによって暗号化される呼びかけメッセージを生成するステップと、

前記呼びかけメッセージを前記第2のハードウェア・エージェントに送信するステップと、

前記第2のハードウェア・エージェントが前記呼びかけメッセージを復号し、前記呼びかけメッセージに応答するステップと、

前記第2のハードウェア・エージェントの前記公開キーによって暗号化される呼びかけメッセージを生成するステップと、

前記第1のハードウェア・エージェントに前記呼びかけメッセージを送信するステップと、

前記第1のハードウェア・エージェントが前記呼びかけメッセージを復号し、前記呼びかけメッセージに応答するステップとをさらに含むことを特徴とする請求項18に記載の方法。

20．転送要求を生成するステップの前に、

前記第2のハードウェア・エージェントが前記有効なライセンス・トークンを所有しているか否かを前記第2のハードウェア・エージェントが判断するステップと、それによって、

前記第2のハードウェア・エージェントが前記有効なライセンス・トークンを所有していない場合には前記通信を終了するステップと、

前記第2のハードウェア・エージェントが前記有効なライセンス・トークンを所有している場合には前記照会メッセージに対する応答メッセージを生成するステップとをさらに含むことを特徴とする請求項16に記載の方法。

**【 発明の詳細な説明】**

ハードウェア・エージェントに対するロビング・ソフトウェア・ライセンス

**発明の背景****発明の分野**

本発明は、ライセンス供与ソフトウェアに関する。詳細には、本発明は、第1のハードウェア・エージェントを有する許可されたノードからライセンス・ソフトウェア・プログラムを実行するアクセス特権を、特定ユーザ・ライセンスに違反することなく第2のハードウェア・エージェントを有する非許可ノードに転送する装置および方法に係わる。

**本発明に関する背景技術**

コンピュータ・システムの発展の初期には、近代化された企業は一般に、メインフレームに接続されたいくつかの「ダム(dumb)」端末を有する、一部屋の大きさの集中メインフレームを使用していた。より小型で高速で高性能のコンピュータの登場と共に、それらの近代化された企業の多くは自社の集中メインフレームを撤去して、いくつかのスタンドアロン型コンピュータ、またはパーソナル・コンピュータの集まりを有し、各ユーザが自分のパーソナル・コンピュータを管理する分散ネットワーク(たとえばローカル・エリア・ネットワーク)を使用する方を選んだ。

この非集中化傾向を認めて、多くのソフトウェア開発業者が「ユーザ特有の」ライセンスと一般に呼ばれる特定のライセンス供与方式に従って自社のソフトウェアをライセンス供与している。ユーザ特有のライセンスは一般に、特定のソフトウェア・プログラムを特定の方式で随時操作することを所定数の個人に許可する。したがって、ライセンスは特定のノードではなく選択された数の個人に付随する。本出願の範囲では、「ノード」とは、好ましくは本発明を含む、コンピュ

ータ、プリンタ、ファクシミリ機、および同様のものなどの「インテリジェンス」を有するハードウェア製品であると定義する。ユーザ特有のソフトウェアに付随する主要な問題は、ソフトウェア開発業者の潜在的ライセンス供与収益をむしろライセンス・ソフトウェアの無許可の使用またはコピーあるいはその両方を

間接的に助長することである。

長年にわたり、ソフトウェア開発業者は、自社のソフトウェアがユーザ特有のライセンスの条件の範囲を超えて使用およびコピーされないように保護する方法を探し求めてきたが、企業ライセンス被供与者は自社の従業員によるライセンス・ソフトウェアの不法な使用またはコピーによる潜在的な代位責任を大幅に軽くしようとしてきた。したがって、ユーザ特有のライセンスの条件を超えたソフトウェアの拡散を防止することは、ソフトウェア開発業者と企業ライセンス非供与者の両方に同様に利益がある。

現在、ユーザ特有のソフトウェア・ライセンスの遵守は、「 dongle ( d o n g l e ) 」と呼ばれる物理的ハードウェア装置の使用によって行われている。 Dongle とは、最初に購入したときにライセンス・ソフトウェアと共にパッケージされている物理ハードウェア装置である。これは一般には、たとえばパーソナル・コンピュータなどのノードの平行・ポートに接続する。実行中の様々な時点で、対象ライセンス・ソフトウェア・プログラムはdongle内で使用されているアクティブ装置に許可メッセージ(「呼びかけ」と呼ばれる)を送る。dongle内のアクティブ装置は、dongle内部に記憶されている秘密情報(以下、「有効ライセンス・トークン」と呼ぶ)を使用してその呼びかけを処理し、戻りメッセージ(「応答」と呼ぶ)を発生する。ソフトウェア・プログラムはこの応答を期待応答と比較し、その2つの応答が同じである場合にのみそれ以降の実行を許可する。

したがって、ユーザはライセンス・ソフトウェア・プログラムをコピーし、それを複数のパーソナル・コンピュータにロードすることはできるが、そのソフトウェア・プログラムを実行することができるのはdongleが接続されている第1のコンピュータのみである。ライセンス・ソフトウェア・プログラムを他のパーソナル・コンピュータで実行するためには、第1のパーソナル・コンピュータか

らdongleを取り外して他のパーソナル・コンピュータに接続しなければならない。その結果、第1のパーソナル・コンピュータではそのソフトウェアは使用不能になる。企業ライセンス被供与者に与えられるdongleの数は一般にユーザ特



有のソフトウェア・ライセンス契約を結んだ人数に限定されているため、ライセンス・ソフトウェア・プログラムの複数の導入がソフトウェア開発業者にとって不利な財務上の影響を引き起こさないことは明らかである。

dongルによってユーザ特有のライセンスの遵守は確保されるが、いくつかの欠点がある。1つの欠点は、dongルを顧客に物理的に配布しなければならないことである。したがって、ソフトウェアの電子配布用システム(「コンテンツ配布」と呼ぶ)が提案され、実施されて便利さを増し、配布コストを削減しているが、物理装置としてのdongルは依然として従来の配布方法とそれに伴う費用とを必要とする。ソフトウェア開発業者の経済的利益を保護するためにdongルを必要とすることによって、顧客は、(i)選定された場所でdongルを直接入手し、その後でそのdongルをノードに装着してからでなければライセンス・プログラムを使用することができないか、または(ii)意図した使用の前にコンテンツ配布者が顧客にdongルを郵送する時間を見越してライセンス・ソフトウェア・プログラムを発注するという煩わしい作業に耐えなければならない。いずれにしても、dongルはコンテンツ配布の効率と興味を妨げる。

もう一つの欠点は、dongルの取り外しと装着が時間のかかる処理であることである。時間を争う企業では、dongルの交換は企業の業績全体に影響を及ぼす。他の欠点は、dongルを絶えず取り外したり装着したりすることによって、dongルが損傷し機能不能になる確率が高くなり、企業は新しいdongルを待ってからでなければ、そのソフトウェア・アプリケーションを再び使用することができない。

他の欠点は、ライセンスは個人を対象としているが、dongルは一般にノードに装着されることである。したがって、ユーザが別の機械(たとえば自宅にあるパーソナル・コンピュータ)に移動した場合、そのユーザはdongルを所有していない限り、ライセンス・ソフトウェア・プログラムを使用することができない。

#### 発明の簡単な概要

上記に基づき、ノード内に内部実装された集積回路構成要素として、電子dong

グルの機能を備えた暗号装置を作製することが望ましい。したがって、本発明の目的は、集積回路構成要素を遠隔認証する際に使用する固有デジタル証明を内部的に記憶する記憶素子を備えた、集積回路構成要素としての暗号装置を提供することである。

本発明の他の目的は、固有の公開キーと私用キーとの対を内部的に生成し、少なくとも秘密キーを記憶することができ、それによって集積回路構成要素の外部の使用を防止する固有集積回路構成要素を提供することである。

本発明の他の目的は、あるエンティティによって検証または製造された別の同様の集積回路構成要素とのセキュリティ保護された通信を可能にするために、そのエンティティの公開キーを内部的に記憶する集積回路構成要素を提供することである。

本発明の他の目的は、ハードウェアの物理的操作を頻繁に必要としないロビング ( r o v i n g ) ・ ソフトウェア・ライセンスを与える集積回路構成要素を提供することである。

この集積回路構成要素を一般にハードウェア・ライセンスと呼び、識別のための動作を行う処理装置と、( i ) 固有の公開キーと私用キーの対を記憶する不揮発性メモリと、( ii) キーの対が認証されたものであるかどうかを検証するデジタル証明と、( iii) 集積回路構成要素と製造業者によって製造された他の同様の構成要素との間の通信を可能にする選定されたエンティティ ( 集積回路構成要素の製造業者であることが好ましい) の公開キーとを含む記憶素子を備える。不揮発性メモリは暗号アルゴリズムを記憶するためにも使用することができる。集積回路構成要素は、処理装置によって処理される情報を記憶する揮発性メモリと、他の同様の構成要素から通信バスを介して暗号化形式または復号形式の情報を送受信するためのインタフェースと、固有の公開キーと私用キーの対を生成するための乱数発生器とをさらに備える。

#### 図面の簡単な説明

本発明の目的、特徴、および利点は以下の本発明の詳細な説明を読めば明らかになる。

第1図は、双方向対称キー暗号化および復号プロセスを示すブロック図である。

第2図は、双方向非対称キー暗号化および復号プロセスを示すブロック図である。

第3図は、信用権威者からのデジタル証明プロセスを示すブロック図である。

第4図は、本発明の実施形態を組み込んだコンピュータ・システムのブロック図である。

第5図は、本発明の実施形態を示すブロック図である。

第6図は、対とデジタル証明を集積回路構成要素に実装する方法を示すフローチャートである。

第7A図～第7C図は、ライセンス特権を有する第2のハードウェア・エージェントと第1のハードウェア・エージェントとの間で有効ライセンス・トークンを転送するために、第1のハードウェア・エージェントが第2のハードウェア・エージェントとの通信を確立する操作を示すフローチャートである。

#### 発明の詳細な説明

本発明は、適切に構成されたハードウェア・エージェント間でロビング・ソフトウェア・ライセンスを転送することができるようにし、それによって配布する物理ハードウェア装置を不要にする装置および方法に関する。以下の説明では、本発明を十分に理解することができるよう多くの詳細を記載する。しかし、当業者には、本発明の精神および範囲から逸脱することなく、本発明を例示されているものとは異なる多くの実施形態を使用して実施することができることが明らかである。他の場合には、本発明を無用に不明瞭にしないために、周知の回路、要素、および同様のものについては詳細には記載しない。

詳細な説明では、特定の特性または品質を説明するためにいくつかの暗号関係の用語を頻繁に使用するが、ここでそれらについて定義する。「キー」とは従来の暗号アルゴリズムの暗号化または復号あるいはその両方のパラメータである。具体的には、キーは $n$ ビットの長さの二進データの順次配置(「ストリング」)

である（ただし「 $n$ 」は任意の数である）。「メッセージ」とは、一連のバス・サイクルで転送される情報（たとえば暗号化キー・アドレスおよびデータ）であると一般に定義される。この情報には、呼びかけや戻り応答が含まれる。「デジタル証明」とは、通信を開始するエンティティに関する情報であると定義され、典型的には広く公開された信用権威者（たとえば銀行、政府機関、同業組合など）によって私用キーを使用して暗号化されたエンティティの公開キーである。「デジタル署名」とは、デジタル証明と類似しているが、送信者ではなくメッセージ自体の認証に使用される。

ここ数年、1つの場所から他の場所にデジタル情報を送信することがますます望まれるようになってきている。その結果、現在、多くのエンティティが暗号技術を使用しており、それによって正当な受信者にとっては明瞭であいまいさがないが不正な受信者には理解できない方式で情報が転送される。一般に、暗号技術は2つの従来の技法のうちの1つに従って機能する。すなわち、対称キー暗号化または非対称（または公開）キー暗号化あるいはそれらの暗号化技術の組合せである。

第1図を参照すると、対称キー暗号技法の実施形態が図示されている。この技法では、同一、すなわち対称な秘密キー（「SK」と符号が付されている）1を使用して、第1のノード10と第2のノード15の間で転送される原メッセージ5を暗号化して暗号化された原メッセージ20を形成し、暗号化された原メッセージ20を復号して原メッセージ5を復元する必要がある。このような暗号化および復号は、たとえばデータ暗号アルゴリズム（より一般には「DES」と呼ばれる）などの周知の従来の暗号アルゴリズムを使用して行われる。原メッセージ5は、(i) 第1のノード10で暗号化され、(ii) 電話回線および同様のものなどの公共領域25を使用して第1のノード10から第2のノード15に転送され、(iii) 第2のノード15で復号される。しかし、この技法は秘密キー（「SK」）を前もって設定する必要があるため、ユーザ数が多い場合にはサポートするのが困難である。

次に第2図を参照すると、非対称キー技法の実施形態が図示されている。この技法は、暗号化と復号に別々に使用される2つの別々のキー（「公開キー」および

び「私用キー」と呼ぶ)を使用する。第1のノード10から第2のノード15への双方向通信を確立するために、第2のノード15のキーの対のうちの「公開」キー16(「PUK2」と符号が付されている)が第1のノード10に記憶され、一般に第1のノード10が暗号化の分野で周知の非対称「RSA」アルゴリズムに基づいて原メッセージ30を暗号化するために使用する。これによって、第2のノード15に転送される暗号化原メッセージ35が形成される。第1のノード10の公開キーと私用キーの対11および12(「PUK1」および「PRK1」と符号が付されている)はさらに第1のノード10に記憶される。

第2のノード15のキーの対のうちの「私用」キー17(「PRK2」と符号が付されている)は、第2のノード15のみが知っており、第2図に示すようにRSAアルゴリズムに基づく第1のノード10からの暗号化メッセージ35の復号を含む多くの目的のために使用する。しかし、この技法は、不正なエンティティ(たとえば商業スパイなど)が正当なエンティティ(たとえば従業員、合併企業など)を装おって、仕事の流れを中断させたり機密情報を入手したりするために他の正当なエンティティに詐欺的メッセージを送信しようとする試みを許しやすい。したがって、一般に付加的なプロトコルを使用して、メッセージの認証を行い、そのメッセージを送信するエンティティの正当化を行う。

事前には未知である当事者間で最初に通信を確立するときは、送信者の認証(すなわち公開キーの送信者が実際にその公開キーの真の所有者であることの検証)が問題である。この問題は、一般に、送信メッセージ50内にデジタル証明45を組み込むことによって回避される。デジタル証明45は、相互信用権威者55(たとえば銀行、政府機関、同業者組合など)が、署名文(「SM」と符号が付されている)58を使用して通信を開始するノードの公開キー(「PUK1」)11を、信用権威者55の私用キー(「PRKTA」)57を使用して暗号化することによって発行する。したがって、PUK2 16を使用しようとする不正な試みが行われてもその送信メッセージに対しては受信者には読めない応答が返されることになるだけである。選択される信用権威者55は、関係当事者によって異なる。たとえば、同じ企業に雇用されている2人の個人は両者とも、その企業の会社セキュリティ管理局によって発行された証明を信用する。しかし

、

2つの独立した企業エンティティの従業員は、それぞれのセキュリティ管理局からの認証だけでなく、たとえばそのような企業エンティティを証明する何らかの産業組織からの証明も必要とする。

この手法では、複数の操作を並列して実行して送信メッセージ50を作成する。1つの操作は、DESアルゴリズムを介して対称秘密キー(「SK」)60を使用して原メッセージ40を暗号化して、デジタル証明45と共に送信メッセージ50に入れられる暗号化メッセージ65を形成することである。原メッセージ40にはハッシュ・アルゴリズム70(たとえば「MD5」)も適用されて、送信メッセージ・ダイジェスト75が形成される。送信メッセージ・ダイジェスト75は、第1のノードの私用キー(「PRK1」)12を使用してさらに暗号化されてデジタル署名80を形成し、それが送信メッセージ50に入れられる。さらに、対称キー(「SK」)60がRSAアルゴリズムに基づいて第2のノードの公開キー(「PUK2」)16を使用して暗号化されて「SKenc」85となり、さらに送信メッセージ50に入れられる。

第3図を続けて参照する。第1のノード10から公共領域25を介して送信される送信メッセージ50を受信すると、第2のノード15は私用キー(「PRK2」)17を使用してSKenc85を復号し、信用権威者55の発行公開キー(「PUBTA」)を使用してデジタル証明45を復号し、SK60とPUK1

11を入手する。このSKキー60とPUK1キー11を使用して、暗号化原メッセージ65とデジタル署名80を復号し、送信メッセージ・ダイジェスト75と原メッセージ40をそれぞれ取り出す。次に、原メッセージ40に第1のノード10で行われたのと同じハッシュ・アルゴリズム85を適用する。その結果90(「受信メッセージ・ダイジェスト」と称する)が、送信メッセージ・ダイジェスト75と比較される。送信メッセージ・ダイジェスト75が受信メッセージ・ダイジェスト90と同じ場合、この2つの正当ノード間の通信が維持される。

第4図を参照すると、本発明を使用するコンピュータ・システム100の実施

形態が図示されている。コンピュータ・システム100は、ホスト・プロセッサ105と、メモリ装置110と、入出力(「I/O」)制御装置115と、「ハードウェア・エージェント」と呼ばれる暗号装置12とを備える。複数のバス・

エージェントがシステム・バス130を介して互いに接続され、それによってこれらのバス・エージェント間で情報を伝達することができる。

この実施形態ではホスト・プロセッサ105しか図示されていないが、コンピュータ業界では周知のように、コンピュータ・システム100内で複数のホスト・プロセッサを使用することもできるものと企図される。さらに、メモリ装置110はダイナミック・ランダム・アクセス・メモリ(「DRAM」)、読取り専用メモリ(「ROM」)、ビデオ・ランダム・アクセス・メモリ(「VRAM」)、および同様のものを含むことができる。メモリ装置110には、ホスト・プロセッサ105が使用する情報が記憶される。

入出力制御装置115は、入出力バス135とシステム・バス130との間のインタフェースであり、システム・バス130または入出力バス135に結合された構成要素間で情報を転送する通信経路(すなわちゲートウェイ)を提供する。入出力バス135はコンピュータ・システム100内の少なくとも1つの周辺装置との間で情報を転送する。これには、画像を表示する表示装置140(たとえば陰極線管、液晶表示装置など)、ホスト・プロセッサ105に情報およびコマンド選択を伝達する英数字入力装置145(たとえば英数字キーボードなど)、カーソル移動を制御するカーソル制御装置150(たとえばマウス、トラックボール、タッチ・パッドなど)、情報を記憶する大容量データ記憶装置155(たとえば磁気テープ、ハード・ディスク・ドライブ、フロッピー・ディスク・ドライブなど)、コンピュータ・システム100から他の装置に情報を送信する情報送受信装置160(ファックス機、モデム、スキャナなど)、および情報の有形の視覚表現を提供するハード・コピー装置165(たとえばプロッタ、プリンタなど)が含まれるがこれらには限定されない。第4図に示すコンピュータ・システムはこれらの構成要素または例示したもの以外の構成要素のうちの一部または全部を使用することができる。

次に、第5図に示す本発明の実施形態を参照すると、ハードウェア・エージェント120は、ホスト・プロセッサ105および、メモリおよび入出力制御装置（図示せず）との通信経路を確立するシステム・バス130に結合されている。ハードウェア・エージェント120は、ダイ121を損傷と有害汚染物質から保

護するように集積回路構成要素パッケージ122内に、好ましくは密閉されてカプセル封止されたダイ121（たとえばマイクロコントローラ）の形態の単一の集積回路を含む。ダイ121は、記憶素子124に結合された処理装置123と、バス・インタフェース125と、乱数発生器126とを含む。バス・インタフェース125は、ハードウェア・エージェント120から他の装置（たとえばホスト・プロセッサ、他の装置内の他のハードウェア・エージェントなど）への通信を可能にする。処理装置123は、ダイ121の中のセキュリティ保護された環境内で内部的に計算を行って、許可された受信者との有効な接続を確認する。そのような計算には、特定のアルゴリズムおよびプロトコルの実行、装置固有の公開／私用キー対および同様のものを生成する、回路（たとえばランダムな性質であることが好ましい、乱数発生器126など）の起動が含まれる。処理装置123は、コンピュータ・システムを混乱させてその私用キーおよびその他の情報を入手する一般的な方法であるウィルス攻撃による私用キーのアクセスを防ぐようにダイ121内に配置されている。

記憶素子124は、「RSA」や「DES」などの適切な暗号アルゴリズム、公開キーと私用キーの対127a、価値の対が認証されたものであるかどうかを検証するためのデジタル証明（「DC」という符号が付されている）127b、および集積回路構成要素とその製造業者によって製造された他の同様の装置との間の通信を可能にする集積回路構成要素の製造業者の公開キー（「PUKM」）127cを記憶するフラッシュ・メモリなどの不揮発性メモリ素子127を含む（第6図に詳細に記載する）。電源が切断されても内容を保持するため、この不揮発性メモリ127が主として使用される。メモリ装置124は、処理装置123からの特定の結果を記憶するためにさらにランダム・アクセス・メモリ（「RAM」）128を含む。



ハードウェア・エージェント 120 は、セキュリティ強化のためにシステム・バス 130 に接続された周辺装置として実装されているが、ハードウェア・エージェント 120 は PC プラットフォーム・レベルで他のいくつかの方法（たとえば、ハード・ディスクから入出力される情報の自動的な復号または暗号化あるいはその両方を行う ディスク制御装置または PC MC I A カードとしてなど）で実

施することもできるものと企図される。他の代替実施態様は、後述するようにハードウェア・エージェントをホスト・プロセッサを含むマルチチップ・モジュールの 1 つの構成要素とすることであろう。さらに、ハードウェア・エージェントについて PC プラットフォームと関連して説明しているが、このようなハードウェア・エージェントはファックス機、プリンタおよび同様のものなどのノード内や、コンピュータと入出力周辺装置との間の通信経路上に実施することもできるものと企図される。

第 6 図を参照すると、本発明を製作する操作のフローチャートが示されている。まず、ステップ 100 で、任意の従来の公知の半導体製造技法に従ってハードウェア・エージェントのダイを製作する。次に、ハードウェア・エージェント自体を形成するようにそのダイを半導体パッケージ内にカプセル封止する（ステップ 105）。証明システム上にハードウェア・エージェントを配置し、それによってハードウェア・エージェントと証明システムとの間に電気的および機械的結合を確立する（ステップ 110）。証明システムは、ハードウェア・エージェントの証明のための電気信号の発生と受信を行う、プリント回路基板に結合されたキャリヤを備える。証明システムはさらに、固有キー生成を保証するために前に生成された公開キーの記憶装置（たとえばデータベース）をさらに備える。その後で、証明システムはハードウェア・エージェントに電力を供給し、ハードウェア・エージェントは乱数発生器に電力を供給してハードウェア・エージェント内で乱数発生器が装置固有の公開キーと私用キーの対を内部的に生成することができるようにする。

ハードウェア・エージェント内で公開キーと私用キーの対が生成された後、公開キーと私用キーの対のうちの公開キーを証明システムに送る（ステップ 120

）。その公開キーを、記憶装置に記憶されている前に製造されたハードウェア・エージェントの前に生成された公開キーと比較する（ステップ125）。万一、その公開キーが前に生成された公開キーの1つと同じである場合（ステップ130）、証明システムがハードウェア・エージェントに対して別の前記公開キーと私用キーの対を生成するように通知し（ステップ135）、このプロセスをステップ120から続けて各公開キーと私用キーの対が確実に固有のものになるようにする。

公開キーが固有である場合は、記憶装置はその固有の公開キーで更新される（ステップ140）。その後、証明システムがステップ145で、キーの対が認証されたものであるかどうかを検証する固有装置証明（以下、「認証装置証明」と呼ぶ）を作成する。認証装置証明は、秘密私用製造業者キーを使用して「デジタル署名」された装置の公開キーを少なくとも含む（すなわち、大ざっぱに言えば製造業者の私用キーを使用して装置の公開キーを暗号化する）。この認証装置証明を製造業者の一般に知られた公開キーと共にハードウェア・エージェントに入力し（ステップ150）、ハードウェア・エージェントは固有公開キーと私用キーの対と認証装置証明と製造業者の公開キーをその不揮発性メモリに永久的にプログラムする（ステップ155）。しかし、製造業者の代わりに他のエンティティ（たとえば配布業者）の公開キーを使用することもでき、その場合は認証装置証明の変更も必要になることが企図される。この時点で、ハードウェア・エージェントは物理的に固有であり、これで他のハードウェア・エージェントとの通信を安全に確立することができる。

ハードウェア・エージェントを製作した後、それを第4図に示すコンピュータ・システムなどの電子装置に実装する。これは、呼びかけ／応答などの認証手続きとその他の周知の手続きを使用してライセンス供与者とハードウェア・エージェントとの間にセキュリティ保護された通信経路を確立することによって行うことができる。通信経路が安全に確保された後、セキュリティ保護された通信リンクを介して有効なライセンス・トークンをハードウェア・エージェントのフラッシュ・メモリにダウンロードする。ハードウェア・エージェント間で転送するの

ではなく、ライセンス・トークンが複数のハードウェア・エージェントに組み込まれて「有効」状態または「無効」状態にあり、それによってライセンス・トークンを有効化または無効化することもできることがさらに企図される。

第7 A 図および第7 B 図を参照すると、2 つのハードウェア・エージェントの認証の相互遠隔識別の実施形態が示されている。ステップ200で、第1のハードウェア・エージェントが組み込まれた「未許可の」第1のノード（すなわち現在はライセンス・ソフトウェア・アプリケーションの操作を許可されていないノード）と、ライセンス・ソフトウェア・アプリケーションを操作することを許可

された第2のハードウェア・エージェントが組み込まれた許可された第2のノードとの間に通信リンクが確立される。この通信リンクは、モデム、ネットワークなどの任意の従来の通信手段を介して確立することができる。第1のハードウェア・エージェントはその固有認証装置証明を含むメッセージを第2のハードウェア・エージェントに出力する（ステップ205）。両方のハードウェア・エージェントの不揮発性メモリに製造業者の公開キー（「PUK1」）がプログラムされているため、第2のハードウェア・エージェントは製造業者の公開キー（「PUK1」）を使用して認証装置証明を復号し、第1のハードウェア・エージェントの公開キーを入手する（ステップ210）。その後、ステップ215～220で、ステップ205～210に記載されているものと同様の操作も行われ、それによって第1のエージェントは第2のハードウェア・エージェントの公開キー（「PUK2」）を入手する。

その後、ステップ225および230で、第2のハードウェア・エージェントが、第1のハードウェア・エージェントの導き出された公開キーを使用して、選定された暗号アルゴリズム（たとえばRSA）に従って呼びかけメッセージを暗号化し、その呼びかけメッセージを第1のハードウェア・エージェントに送信する。ステップ235および240で、第1のハードウェア・エージェントが、その私用キー（「PRK1」）を使用して呼びかけメッセージを復号し、次に、復号した呼びかけメッセージを第2のハードウェア・エージェントの公開キー（「PUK2」）を使用して暗号化することによって応答メッセージを生成し、その

応答メッセージを第2のハードウェア・エージェントに送信する。次に、第2のハードウェア・エージェントが、前に送信された製造業者の装置証明の復号によって前に判断したその私用キー(「P U K 1」)を使用してその応答を復号する(ステップ245)。ステップ250で、第2のハードウェア・エージェントは元の呼びかけメッセージを、復号した応答メッセージと比較し、同じでない場合は通信を終了する(ステップ255)。同じ場合は、ステップ260~290でステップ225~260と同様の呼びかけ/応答手続きが行われて、第1のハードウェア・エージェントから送信された情報を第2のハードウェア・エージェントが実際に受信していることを検証する。これらのステップ(ステップ22

5~290)が成功裏に完了すると、両方のハードウェア・エージェントが認証されたエージェントであり、両者の間の通信がセキュリティ保護されていることが保証される(ステップ295)。

次に第7C図を参照すると、セキュリティ保護された通信のもとで第2のハードウェア・エージェント内の有効なライセンス・トークンを第1のハードウェア・エージェントに安全に転送するプロセスの実施形態が示されている。安全保護された通信が確立されると、第1のハードウェア・エージェントは第2のハードウェア・エージェントに対して有効なライセンス・トークンを所有しているかどうか照会する(ステップ300)。第2のハードウェア・エージェントが組み込まれているシステムが有効なライセンス・トークンを持っていない場合(ステップ305)、ハードウェア・エージェント間の通信は終了する(ステップ310)。しかし、第2のハードウェア・エージェントが組み込まれたシステムが有効なライセンス・トークンを持っている場合は、第1のハードウェア・エージェントにしかるべくメッセージを送信する(ステップ315)。

第1のハードウェア・エージェントは、このメッセージを受信すると、第1のハードウェア・エージェントにライセンス・ソフトウェア・アプリケーションの操作を許す有効なライセンス・トークンの転送要求を出す(ステップ320)。第2のハードウェア・エージェントは、有効なライセンス・トークンを転送することによって転送要求に応答し、それによってそのライセンス特権を失う(ステ

ップ325)。第1のハードウェア・エージェントはその有効なライセンス・トークンを受け取り、そのトークンをその不揮発性メモリに記憶した後、有効なライセンス・トークンを受け取ったというメッセージを第2のハードウェア・エージェントに送信し、そのライセンス・ソフトウェアのコピーを使用可能にすることになる(ステップ330)。この時点で、通信が終了する(ステップ335)。

ステップ320と325の間およびステップ325と330の間に呼びかけ／応答シーケンスを導入することによって、追加のレベルのプロトコル保全性を得ることができることが企図される。これによって、前のライセンス・トークン転送事象の「再生」が防止される。

第1と第2のハードウェア・エージェント間の通信と並行して、各ハードウェア・エージェントはその送信の内容を監査ログとして不揮発性メモリに記憶する。したがって、第2のハードウェア・エージェントがそのコピーを使用不能にした後で第1のハードウェア・エージェントがそのコピーを使用可能にする前に通信が切断された場合、両方のハードウェア・エージェントは通信が再接続された後で監査ログを見直してどのハードウェア・エージェント(ある場合)がライセンス・ソフトウェア・アプリケーションを操作する許可を持っているかを判断することができる。

本明細書に記載の本発明は多くの異なる方法で多くの異なる構成を使用して設計することができる。本発明について様々な実施態様に関して説明したが、当業者なら本発明の精神および範囲から逸脱することなく他の実施態様を考えつくであろう。したがって、本発明は請求の範囲の記載によって判断されるべきである。

【 図 1 】

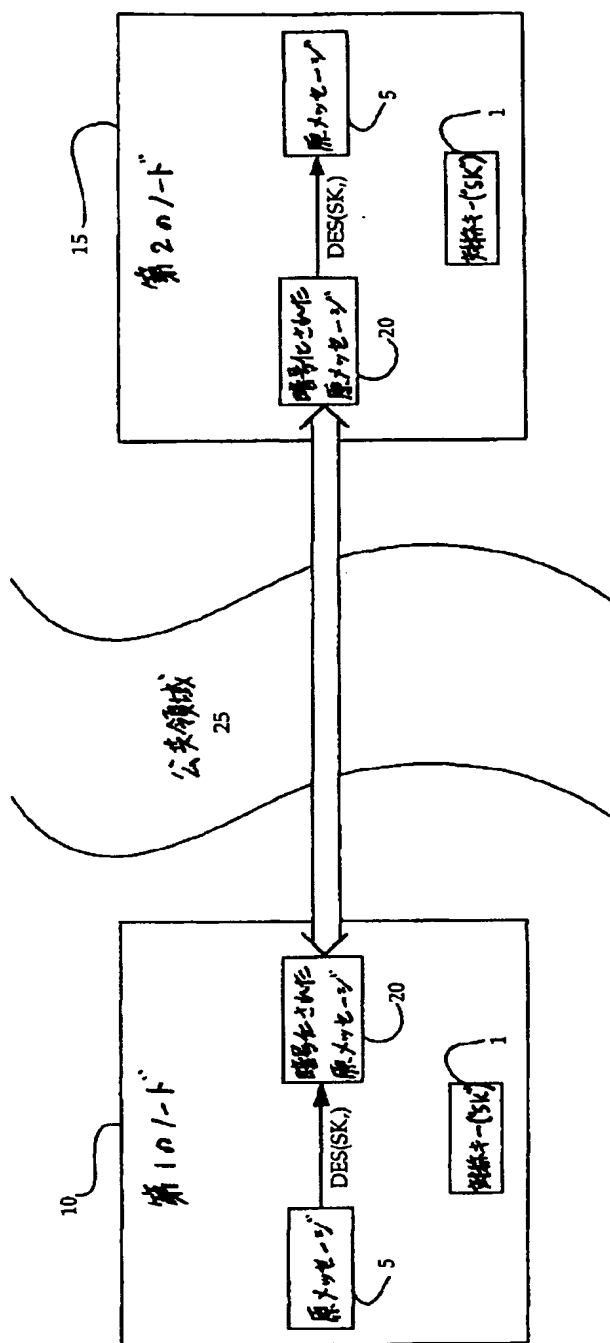


Figure 1

【 図2 】

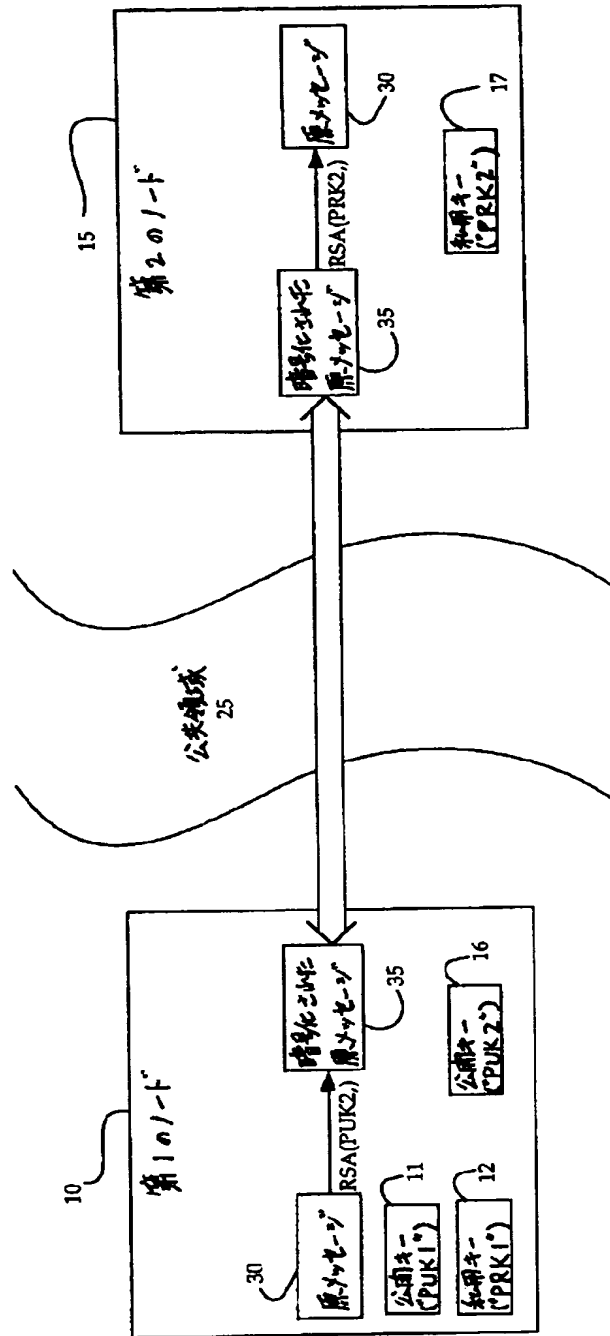


Figure 2

【 図3 】

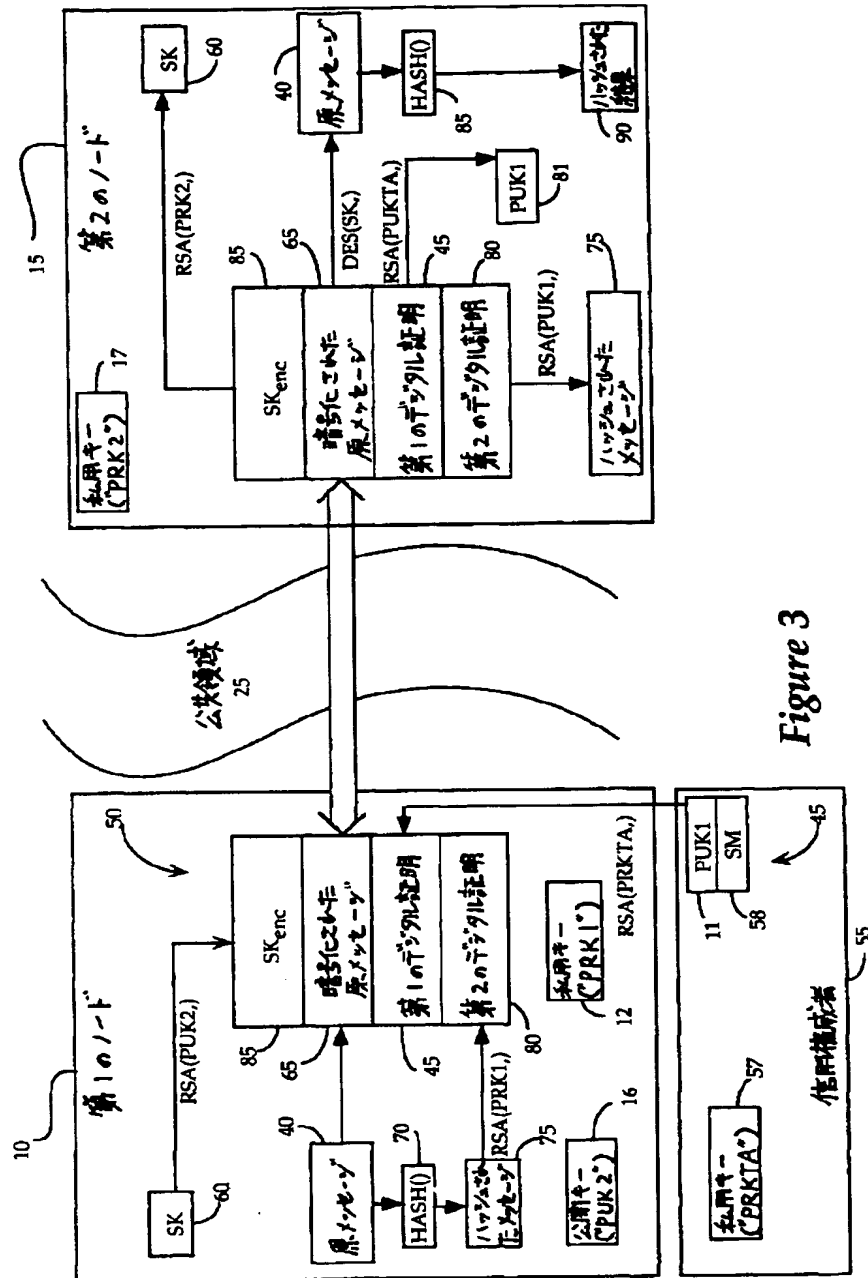
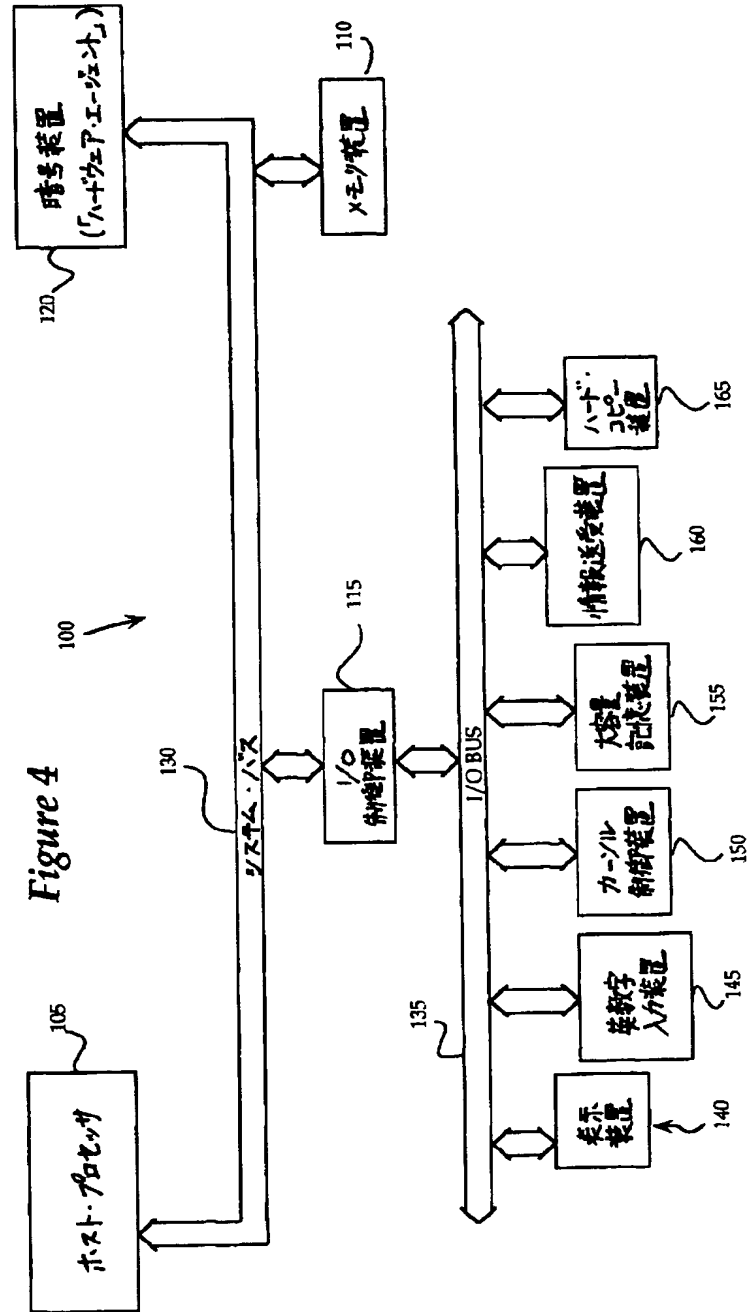


Figure 3



【 図4 】



【 図5 】

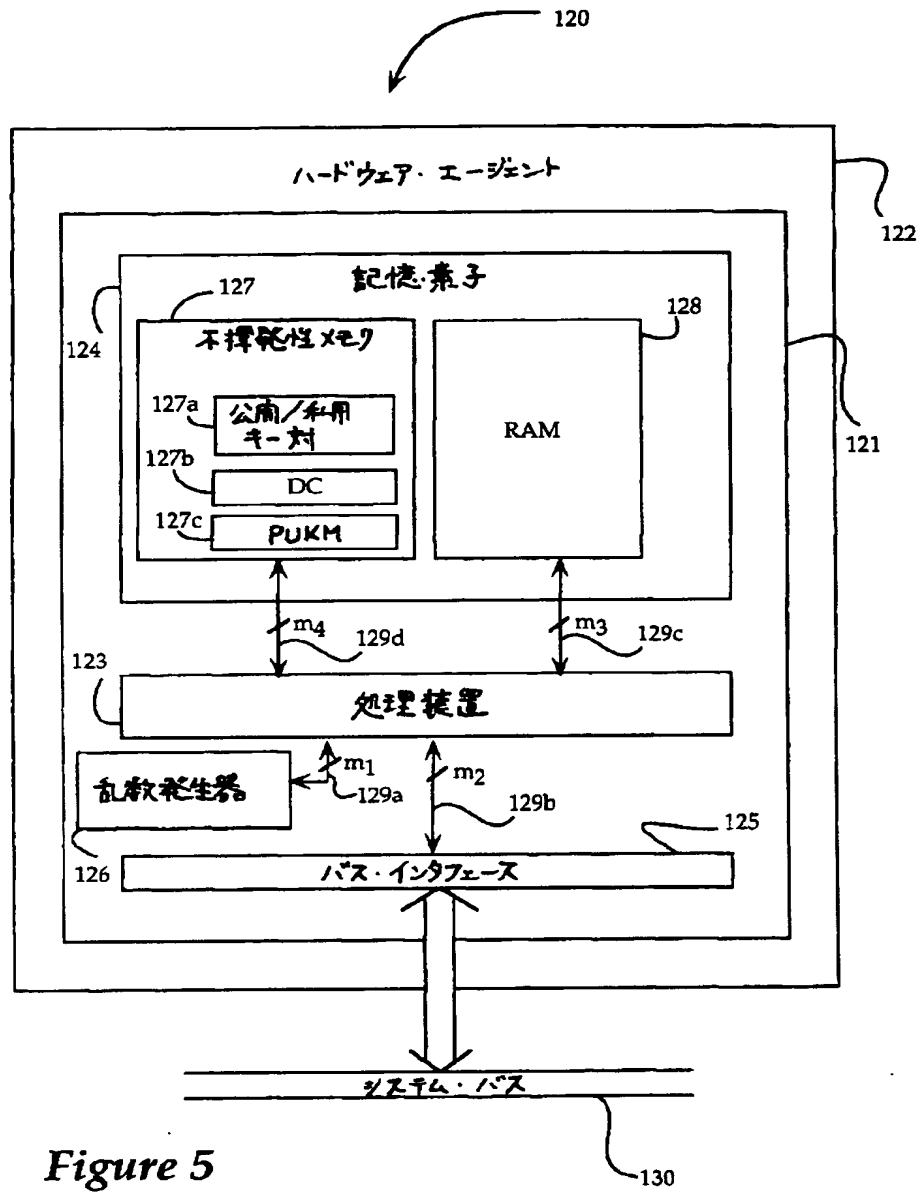


Figure 5

【 図6 】

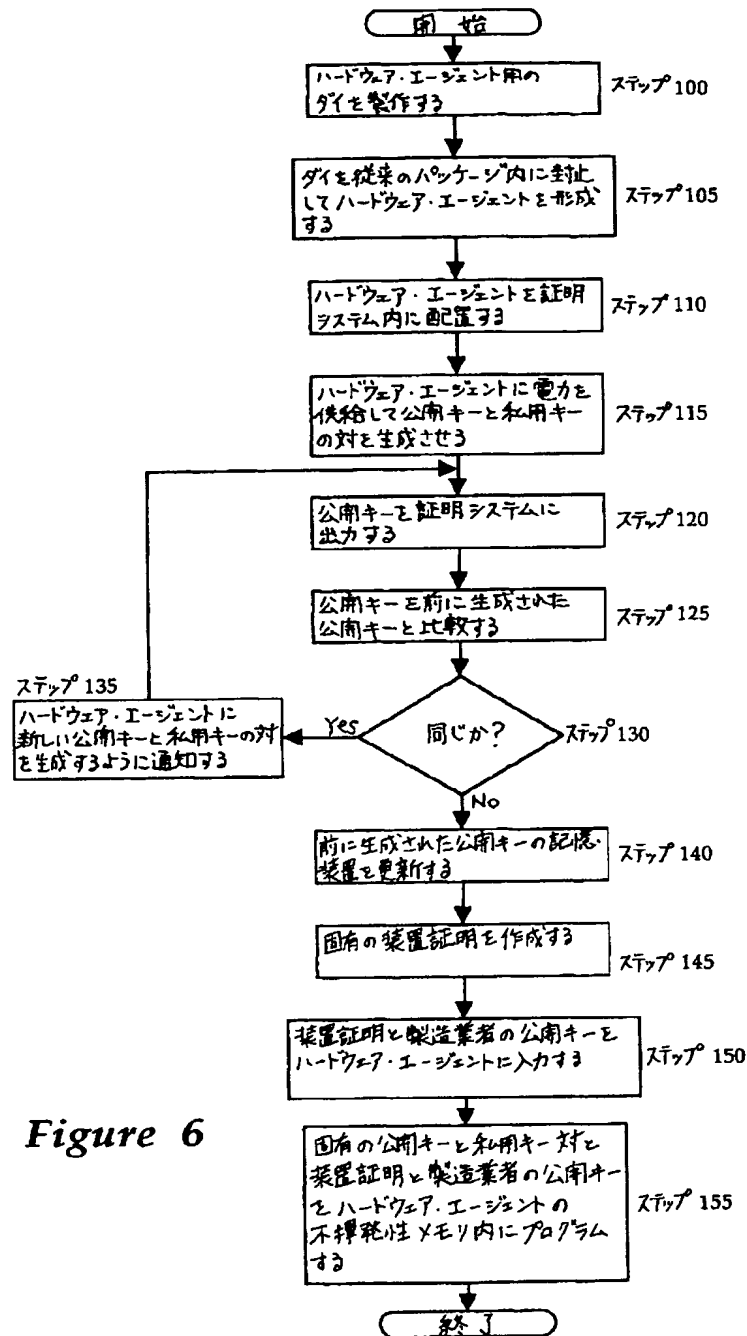


Figure 6

【 図 7 】

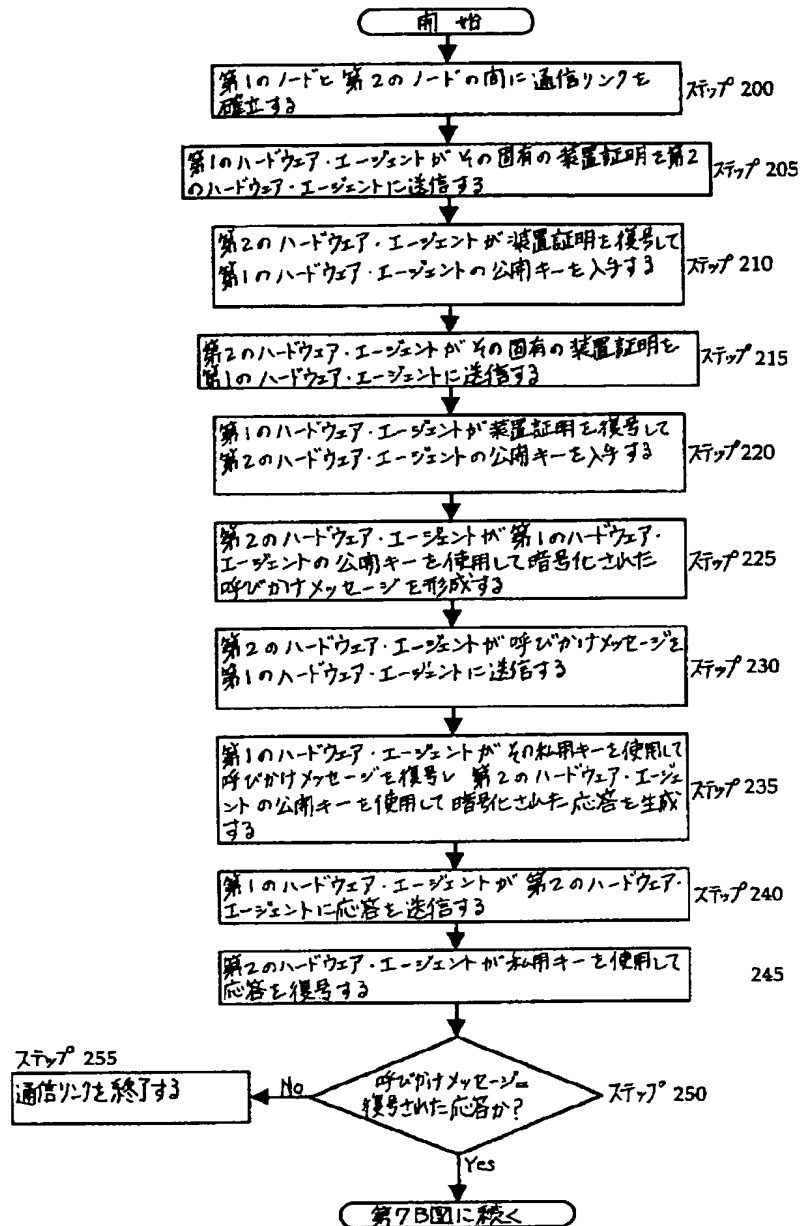


Figure 7A

【 図 7 】

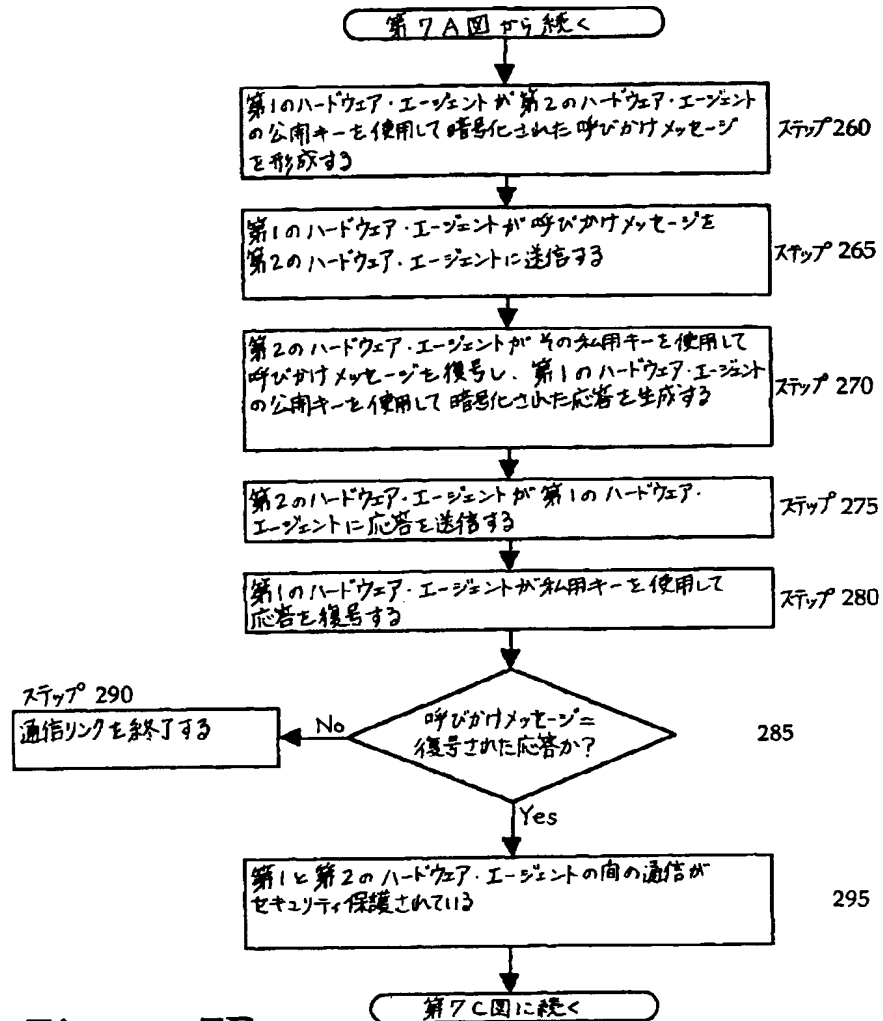


Figure 7B

【 図 7 】

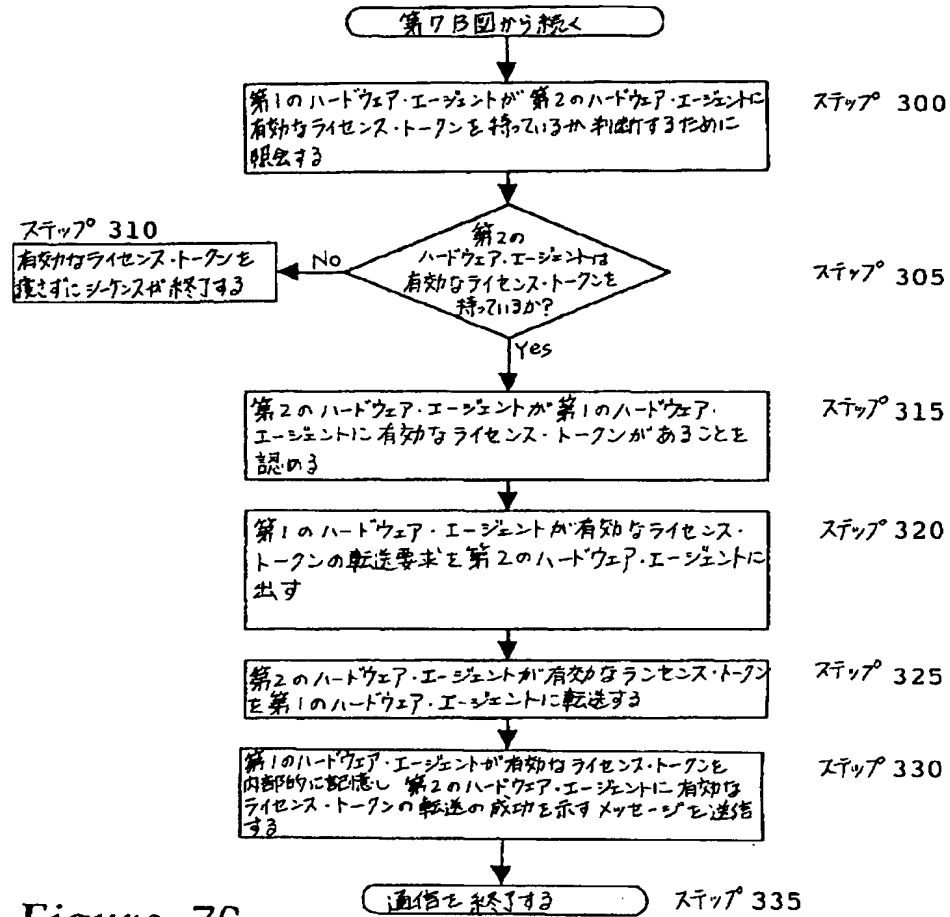


Figure 7C

## 【 国際調査報告 】

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US95/11136

<b>A. CLASSIFICATION OF SUBJECT MATTER</b>				
IPC(6) : H04K 1/00				
US CL : 380/25, 4, 23, 30				
According to International Patent Classification (IPC) or to both national classification and IPC				
<b>B. FIELDS SEARCHED</b>				
Minimum documentation searched (classification system followed by classification symbols)				
U.S. : 380/25, 4, 23, 24, 30				
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched				
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)				
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>				
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.		
A	US, A, 4,807,288 (UGON, ET AL). 21 February 1989	1-20		
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.				
<table border="0"> <tr> <td> <p>* Special categories of cited documents:</p> <p>*A* document defining the general state of the art which is not considered to be of particular relevance</p> <p>*B* earlier documents published on or after the international filing date</p> <p>*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>*O* document referring to an oral disclosure, use, exhibition or other means</p> <p>*P* document published prior to the international filing date but later than the priority date claimed</p> </td> <td> <p>*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>*A* document member of the same patent family</p> </td> </tr> </table>			<p>* Special categories of cited documents:</p> <p>*A* document defining the general state of the art which is not considered to be of particular relevance</p> <p>*B* earlier documents published on or after the international filing date</p> <p>*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>*O* document referring to an oral disclosure, use, exhibition or other means</p> <p>*P* document published prior to the international filing date but later than the priority date claimed</p>	<p>*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>*A* document member of the same patent family</p>
<p>* Special categories of cited documents:</p> <p>*A* document defining the general state of the art which is not considered to be of particular relevance</p> <p>*B* earlier documents published on or after the international filing date</p> <p>*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>*O* document referring to an oral disclosure, use, exhibition or other means</p> <p>*P* document published prior to the international filing date but later than the priority date claimed</p>	<p>*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>*A* document member of the same patent family</p>			
Date of the actual completion of the international search		Date of mailing of the international search report		
13 DECEMBER 1995		21 FEB 1996		
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231		Authorized officer <i>David Cain</i>		
Facsimile No. (703)305-3230		DAVID CAIN		
		Telephone No. (703) 306-1136		

---

フロント ページの続き

(81)指定国           EP (AT, BE, CH, DE,  
DK, ES, FR, GB, GR, IE, IT, LU, M  
C, NL, PT, SE), OA (BF, BJ, CF, CG  
, CI, CM, GA, GN, ML, MR, NE, SN,  
TD, TG), AP (KE, MW, SD, SZ, UG),  
AM, AT, AT, AU, BB, BG, BR, BY, C  
A, CH, CN, CZ, CZ, DE, DE, DK, DK  
, EE, ES, FI, FI, GB, GE, HU, IS,  
JP, KE, KG, KP, KR, KZ, LK, LR, L  
T, LU, LV, MD, MG, MK, MN, MW, MX  
, NO, NZ, PL, PT, RO, RU, SD, SE,  
SG, SI, SK, SK, TJ, TM, TT, UA, U  
G, UZ, VN